Data Breach Response Plan

Barrowby Parish Council

Date Adopted: [Insert Date]

Review Date: [Insert Date + 1 year]

1. Purpose

This document outlines the procedure Barrowby Parish Council must follow in the event of a personal data breach. It ensures prompt action is taken to limit damage, comply with the UK GDPR, and protect the rights of individuals.

2. Definition of a Data Breach

A personal data breach is a security incident that results in:
- Loss, destruction, or corruption of personal data
- Unauthorised access, disclosure, or alteration
- Data being accidentally or unlawfully accessed or shared

Examples include:
- Sending personal data to the wrong recipient
- Lost or stolen devices containing personal data
- Malware or ransomware attacks
- Unauthorised access to council files

3. Roles and Responsibilities

Role	Responsibility
Clerk / Assistant Clerk	Initial breach assessment and documentation
Data Protection Officer (if appointed)	Advise on reporting, mitigation and notification duties
Council Chair	Escalation of severe breaches and communication with ICO/legal bodies
Councillors/Staff	Must report any suspected breach immediately to the Clerk

4. Initial Response Procedure

Step	Action

1	Identify and Contain the breach (e.g., disconnect affected systems, retrieve sent emails)
2	Assess the Risk: What data is involved? How many individuals? Is the data sensitive?
3	Notify the Clerk or DPO immediately. Complete the Breach Report Form.
4	Mitigate: Change passwords, isolate compromised data, secure backups.
5	Evaluate if ICO Notification is Required (see Section 5).

5. Reporting to the ICO

Barrowby Parish Council must report to the Information Commissioner's Office (ICO) within 72 hours if the breach:
- Could result in a risk to the rights and freedoms of individuals (e.g., financial loss, distress, identity theft)

If unsure, it is safer to report than not.

ICO Reporting Form: https://ico.org.uk

6. Notification to Individuals

Individuals must be notified without delay if the breach is high risk, such as:
- Identity theft
- Discrimination
- Significant distress or harm

Notification must include:
- What happened
- What data was affected
- How they can protect themselves
- Who to contact for help

7. Record Keeping

All breaches—whether reported or not—must be recorded in the Data Breach Log, including:
- Description of breach
- Date discovered
- Action taken

- Whether the ICO was informed
- Lessons learned

8. Prevention and Training

- All staff and councillors will be trained on data protection responsibilities.
- Regular reviews of policies and procedures will take place.
- Security controls (e.g., password policies, access controls) will be updated.

9. Review and Audit

This policy will be reviewed annually or after any serious incident. Lessons learned will be incorporated into updated procedures.